WHAT IS CLAIMED IS:

1. A secure token for use with an encrypted file and an insecure decryption device, the secure token comprising a processor for protecting a first cryptographic key against unauthorized access, and creating a second cryptographic key from the first key and a message unique to the insecure device, the second key usable for file decryption by the insecure device.

2. The secure token of claim 1, wherein the secure token includes a smart card, the smart card including the processor.

3. The secure token of claim 1, wherein the processor uses a hash function to create the second key from the message and the first key.

4. The secure token of claim 1, wherein the secure token performs an electronic transaction to obtain the first key.

5. The secure token of claim 4, wherein the secure token conducts a transaction with a server to purchase a desired file; and wherein the secure token receives the first key from the server.

6. The secure token of claim 4, wherein the secure token conducts a transaction with a peer to purchase a file; and wherein the secure token receives the first key from the peer.

7. The secure token of claim 4, wherein the secure token conducts a transaction with a peer to sell a file; and wherein the secure token sends the first key to the peer.

8. The secure token of claim 7, wherein the secure token creates a third key that is unique to the peer, and sends the third key to the insecure device and the peer.

9. The secure token of claim 1, further comprising means for receiving the first key and encrypted data, wherein the insecure device uses the second key to decrypt the encrypted data. C9, ln 42-52: playback decodes content w/ CDK

10. The secure token of claim 1, wherein processing power of the secure token is significantly less than processing power of the insecure device.

C4, ln 23-27

11. An article for a secure device, the secure device including a processor, the secure device used in combination with an insecure device, the article comprising memory encoded with data for instructing the processor to protect a first cryptographic key against unauthorized access, use a hash function to create a second cryptographic key from the first key and a message unique to the insecure device, and send the second key to the insecure device.

12. The article of claim 11, wherein data further instructs the processor to perform an electronic transaction to obtain the first key.

13. The article of claim 12, wherein the secure device conducts a transaction with a server to purchase a desired file; and wherein the secure device receives the first key from the server.

14. The article of claim 13, wherein the secure device conducts a transaction with a peer to purchase a file; and wherein the secure device receives the first key from the peer.

15. The article of claim 13, wherein the secure device conducts a transaction with a peer to sell a file; and wherein the secure device sends the first key to the peer.

16. The article of claim 15, wherein the data further instructs the processor to create a third key that is unique to the peer, sends the third key to the insecure device and the peer.

17. A data rights management server for use with a media transaction system, the server comprising a processing unit programmed to cause the server to establish a secure channel with a smart card, access a unique identifier corresponding to an insecure device, send the first cryptographic key to the smart card via the secure channel, receive a unique identifier from the insecure device, create a second key from the first key and the identifier; encrypt a media file with the second key, and send the encrypted media file to the insecure device, the first key corresponding to the media file.

18. The server of claim 17, wherein the smart card and the server perform an electronic transaction for the first key.

19. A method of using an insecure decryption device for file distribution, the method comprising:

accessing a message unique to the insecure device;

accessing a first cryptographic key;

creating a second cryptographic key from the message and the first key; and

allowing the insecure device to access the second key but not the first key;

whereby the insecure device can use the second key for decryption.

20. The method of claim 19, wherein a hash function is used to create the second key from the message and the first key.

21. The method of claim 19, wherein accessing the first key includes performing an electronic transaction to obtain the first key.

22. The method of claim 21, wherein the electronic transaction is conducted with a server to purchase a desired file; and accessing the first key includes receiving the first key from the server.

23. The method of claim 21, wherein the electronic transaction is conducted with a peer to purchase a file; and wherein accessing the first key includes receiving the first key from the peer.

24. The method of claim 21, wherein the electronic transaction is conducted with a peer to sell a file; the method further comprising sending the first key to the peer.

25. The method of claim 24, further comprising creating a third key that is unique to the peer, and sending the third key to the insecure device and the peer.

26. An insecure decryption device for use with a secure device and a first cryptographic key, the device comprising:

means for sending a message to the secure device, the message unique to the insecure device;

means for receiving a second cryptographic key from the secure device, the second cryptographic key derived from the message and the first cryptographic key; and

means for performing decryption with the second cryptographic key.

27. The device of claim 26, further comprising means for playing media decrypted with the second cryptographic key.

28. A trusted system for file distribution, the system comprising:

an insecure device; and

a trusted secure device for storing a first cryptographic key, accessing a message from the insecure device, creating a second cryptographic key from the message and the first key, and allowing the insecure device to access the second key, the first key granting file access rights;

the insecure device not allowed to access the first key, the insecure device using the second key for decryption.

29. The system of claim 28, wherein the message is unique to the insecure device. (Cl 8, ln 28 – 21)

30. The system of claim 28, wherein the secure device is a secure token. (las)

31. The system of claim 30, wherein the secure token includes a smart card.

32. The system of claim 31, wherein the insecure device includes a media player.

33. The system of claim 28, wherein the secure device is configured to perform an electronic transaction to obtain the first key.

34. The system of claim 28, wherein processing power of the secure device is significantly less than processing power of the insecure device.

35. The system of claim 28, further comprising a peer-to-peer application for identifying peers having desired files. (Cl 9, ln 9–15)

36. A trusted media transaction system comprising

an insecure media player; and

a trusted secure token for performing an electronic transaction to obtain a first cryptographic key, accessing a message from the insecure device, creating a second cryptographic key from the message and the first key, and allowing the insecure device to access the second key, the first key granting media file access rights;

the insecure device configured to use the second key for media file decryption.